

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-313341

(43)Date of publication of application : 24.11.1998

(51)Int.Cl.

H04L 12/56

G06F 13/00

H04L 12/24

H04L 12/26

H04L 29/14

(21)Application number : 10-058104

(71)Applicant : NATL AEROSPACE LAB
KAGAKU GIJUTSU SHINKO
JIGYODAN

(22)Date of filing : 10.03.1998

(72)Inventor : FUJITA NAOYUKI

(30)Priority

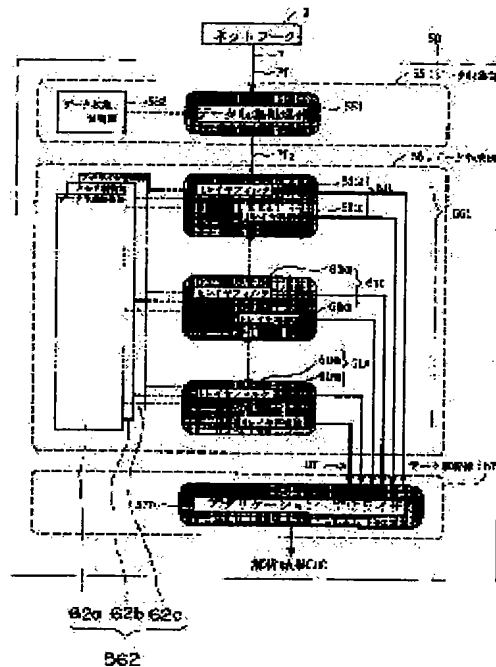
Priority number : 09 56715 Priority date : 11.03.1997 Priority country : JP

(54) METHOD FOR ANALYZING ILLEGAL COMMUNICATION ON NETWORK, SYSTEM FOR ANALYZING ILLEGAL COMMUNICATION ON NETWORK USING THE METHOD, AND RECORDING MEDIUM READABLE BY COMPUTER RECORDING NETWORK ILLEGAL COMMUNICATION ANALYSIS PROGRAM

(57)Abstract:

PROBLEM TO BE SOLVED: To enable a system to handle optional data, to handle optional communication between networks, to facilitate coping with the increase in number of protocols and to handle arbitrary protocols.

SOLUTION: This network illegal communication analysis system 50 analyzes illegal communication on a network, where communication is conducted between information communication stations according to a hierarchical protocol. The system 50 consists of a data collection section 55 that receives a packet PT transmitted on the network 3, a data generating section 56 that sets a parameter of a hierarchical module in response to the hierarchical protocol, based on information in a configuration file read in advance and processes a packet from the data collection section with each hierarchical module to generate analysis data DT, and a data analysis section 57 that discriminates the response of illegal communication in the analysis data DT, based on the content described on the file.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-313341

(43) 公開日 平成10年(1998)11月24日

(51) Int.Cl.⁵ 識別記号

H 0 4 L 12/56

G 0 6 F 13/00 3 5 1

H 0 4 L 12/24

12/26

29/14

F I

H 0 4 L 11/20

G 0 6 F 13/00

H 0 4 L 11/08

13/00

1 0 2 Z

3 5 1 Z

3 1 3

審査請求 有 請求項の数 3 O L (全 15 頁)

(21) 出願番号 特願平10-58104

(22) 出願日 平成10年(1998) 3 月10日

(31) 優先権主張番号 特願平9-56715

(32) 優先日 平 9 (1997) 3 月11日

(33) 優先権主張国 日本 (J P)

(71) 出願人 391037397

科学技術庁航空宇宙技術研究所長
東京都調布市深大寺東町 7 丁目44番地 1

(71) 出願人 396020800

科学技術振興事業団
埼玉県川口市本町 4 丁目 1 番 8 号

(72) 発明者 藤田 直行

東京都小金井市前原町 4 - 17 - 28

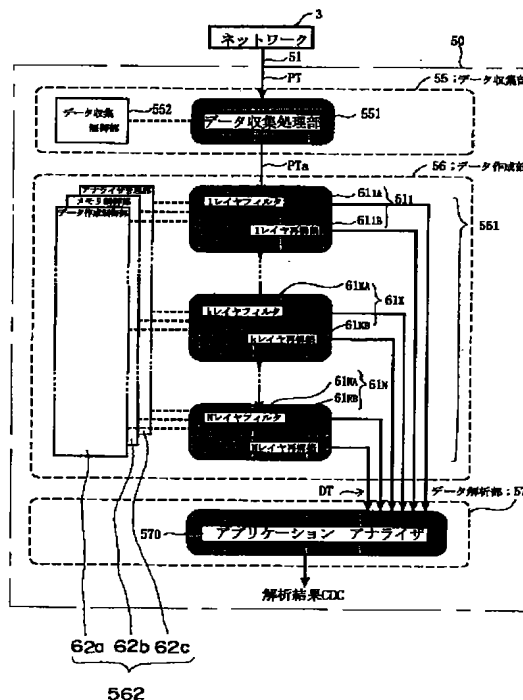
(74) 代理人 弁理士 村瀬 一美

(54) 【発明の名称】 ネットワーク不正解析方法及びこれを利用したネットワーク不正解析装置並びにネットワーク不正解析プログラムを記録したコンピュータ読み取り可能な記録媒体

(57) 【要約】

【課題】 任意のデータを取り扱え、ネットワーク間の任意の通信を扱えて、プロトコル数の増大に容易に対処でき、任意のプロトコルを取り扱うことができるようにする。

【解決手段】 ネットワーク不正解析システム 50 は、情報通信ステーションの間で階層化されたプロトコルにより通信を行うネットワークでの不正を解析するものである。このシステム 50 は、ネットワーク 3 上で伝送されているパケット P T を取り込むデータ収集部 55 と、階層化されたプロトコルに応じた階層化モジュールのパラメータを予め読み込んでおいたコンフィグレーションファイルでの情報に基づいて設定し、データ収集部からのパケットを各階層化モジュールで処理し解析データ D T を作成するデータ作成部 56 と、同ファイルに記載された内容を基に解析データ D T に不正発生の有無を判定するデータ解析部 57 とからなる。



【特許請求の範囲】

【請求項1】 情報通信ステーションの間で階層化されたプロトコルにより通信を行うように構築されたネットワークにおける不正を解析する方法であって、前記ネットワーク上で伝送されているパケットを取り込むデータ収集工程と、階層化されたプロトコルに応じた階層化モジュールのパラメータを予め読み込んでおいたコンフィグレーションファイルで指定された情報に基づいて設定し、前記データ収集工程からのパケットを前記各階層化モジュールでフィルタリングして前記パケットの細分化されたデータを元の単位に再構築することにより解析データを作成するデータ作成工程と、予め読み込んでおいたコンフィグレーションファイルで指定された内容を基に前記データ作成工程からの解析データに不正が発生しているか判定するデータ解析工程とを備えたことを特徴とするネットワーク不正解析方法。

【請求項2】 情報通信ステーションの間で階層化されたプロトコルにより通信を行うように構築されたネットワークにおける不正を解析する装置であって、前記ネットワーク上で伝送されているパケットを取り込むデータ収集部と、階層化されたプロトコルに応じた階層化モジュールのパラメータを予め読み込んでおいたコンフィグレーションファイルで指定された情報に基づいて設定し、前記データ収集部からのパケットを前記各階層化モジュールでフィルタリングして前記パケットの細分化されたデータを元の単位に再構築することにより解析データを作成するデータ作成部と、予め読み込んでおいたコンフィグレーションファイルで指定された内容を基に前記データ作成部からの解析データに不正が発生しているか判定するデータ解析部とを備えたことを特徴とするネットワーク不正解析装置。

【請求項3】 情報通信ステーションの間で階層化されたプロトコルにより通信を行うように構築されたネットワーク上で伝送されているパケットを取り込むデータ収集手順と、階層化されたプロトコルに応じた階層化モジュールのパラメータを予め読み込んでおいたコンフィグレーションファイルで指定された情報に基づいて設定し、前記データ収集手順からのパケットを前記各階層化モジュールでフィルタリングして前記パケットの細分化されたデータを元の単位に再構築することにより解析データを作成するデータ作成手順と、予め読み込んでおいたコンフィグレーションファイルで指定された内容を基に前記データ作成手順からの解析データに不正が発生しているか判定するデータ解析手順とをコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明はネットワーク不正解析方法及びこれを利用した装置並びにネットワーク不正

解析プログラムを記録したコンピュータ読み取り可能な記録媒体に関する。さらに詳述すると、本発明は、情報通信ステーションの間で階層化されたプロトコルにより通信を行うように構築されたネットワークにおいて通信されるデータに不正が発生しているか否かを解析しネットワークのセキュリティやネットワーク管理を実行できるネットワーク不正解析方法及びこれを利用した装置並びにネットワーク不正解析プログラムを記録したコンピュータ読み取り可能な記録媒体に関するものである。

【0002】 本明細書中では、ネットワークにおける「不正」とは例えばクラッキング等のいわゆる不正アクセスを意味する。

【0003】

【従来の技術】 従来、情報ステーションの間でデータの交換を行うように構成されたシステムにおいて、交換されるデータに不正が発生しているか否かを解析する解析方法が種々提供されている。

【0004】 まず、上記解析方法の第1の従来技術としては、例えば7層モデルのトランスポート層（トランスポートレイヤ）上に位置して動作し、トランスポートレイヤから通信内容を受け取り、オペレーティングシステムが用意している関数により、発信元をチェックし予め登録してある許可されるべき発信元かどうかの判定をするようにした解析システムが提案されている（TCP WRAPPER；Mar19 1996）。

【0005】 また、上記解析方法の第2の従来技術としては、ネットワーク通信の機能を使用しないソフトウェアであって、所定の圧縮方法を用いて膨大なハードディスクの内容を圧縮しておき、定期的に保存してある内容と現在の圧縮した内容が一致するか否か比較することによりハードディスクへの不正なアクセスを検知するものがある（The Design and Implementation of Tripwire；Feb 23 1995）。

【0006】 さらに、上記解析方法の第3の従来技術としては、典型的な不正（クラッキング（Cracking））手法が格納されていて、その手法を解析対象のシステムに対して実行することにより、当該システムの不正をチェックするようにしたものがある（Satan-network security scanner）。

【0007】 また、上記解析方法の第4の従来技術としては、ネットワーク通信そのものより、ネットワーク通信によってクラッキングされてしまう設定になっていないかどうかをホストコンピュータ毎に解析するものであって、ホストコンピュータのさまざまな設定内容がセキュリティ的に危険なものでないかオペレーティングシステムのコマンドを用いてチェックを行うようにしたものがある（COPS；Nov 171991）。

【0008】 上記解析方法の第5の従来技術としては、UNIXで用いられているユーザのパスワードが妥当なものであるかどうかをチェックするものであって、パス

ワードの候補ファイルをもって候補の単語を暗号化し、暗号化した結果作成された暗号化された単語と暗号化されているパスワードとを比較し、一致すればいま暗号化した単語がパスワードであることを利用してパスワードの検索をおこなうようにしたシステムがある（Crack Version 4.1 ; Mar 3 1992）。

【0009】上記解析方法の第6の従来技術としては、物理層パケット単位の解析を行うものがある（Sniffer）。

【0010】さらに、上記解析方法の第7の従来技術としては、階層化されたプロトコルにより情報ステーション間の通信を行うネットワークの診断システムであって、下位のレイヤフィルタから提供されたサービスデータユニットを入力制御からの解析指示に従って解析するとともに、上位のレイヤフィルタに対するサービスデータユニットを作成して提供するようにしたものがある（特開平4-315343号公報）。

【0011】

【発明が解決しようとする課題】しかしながら、上記第1の従来技術によれば、トランスポートレイヤからデータを受け取るのみで、他のレイヤからデータを受けるものではないため、解析するデータが少なく不正の解析に十分ではない欠点がある。また、オペレーティングシステムの機能によりデータの再構築を行っているため、不正の解析に十分ではないという欠点がある。

【0012】上記第2の従来技術によれば、ネットワーク通信機能を有していないため、ネットワーク通信のデータの不正解析ができないという欠点があった。

【0013】さらに、これら第1、2の従来技術によれば、監視対象ホストコンピュータやホストステーション（以下、単に「ホスト」という）毎に当該解析方法を実現するプログラムをインストールする設計となっているため、ホスト数の増大に対応できない。

【0014】そして、上記第3～5の従来技術によれば、解析プロトコル毎に新たな解析を行う設計となっているため、プロトコル数の増大に対応できない。

【0015】また、上記第6の従来技術によれば、物理層パケット単位の解析を行う設計となっているため、クラッキング解析に不可欠なアプリケーション層セッション単位の解析ができない。

【0016】一方、上記第7の従来技術によれば、プロトコルの各レイヤ毎に同一モジュールで当該レイヤ部分のデータのフィルタリングと診断とをおこなうようになっているため、他のレイヤとの関連で不正を解析することができず、不正の解析が十分とはいえないという欠点があった。

【0017】そこで、本発明の第1の目的は、アプリケーションのセッションを含め任意のデータを取り扱うことができるネットワーク不正解析方法及びこの方法を利用したネットワーク不正解析装置並びにネットワーク不

正解析プログラムを記録したコンピュータ読み取り可能な記録媒体を提供することにある。

【0018】また、本発明の第2の目的は、ネットワーク間の任意の通信を扱うとともに、プロトコル数の増大に容易に対処できるネットワーク不正解析方法及びこの方法を利用したネットワーク不正解析装置並びにネットワーク不正解析プログラムを記録したコンピュータ読み取り可能な記録媒体を提供することにある。

【0019】さらに、本発明の第3の目的は、任意のプロトコルを取り扱うことができるネットワーク不正解析方法及びこの方法を利用したネットワーク不正解析装置並びにネットワーク不正解析プログラムを記録したコンピュータ読み取り可能な記録媒体を提供することにある。

【0020】

【課題を解決するための手段】上記第1～第3の目的を達成するため、請求項1記載の発明は、情報通信ステーションの間で階層化されたプロトコルにより通信を行うように構築されたネットワークにおける不正を解析するネットワーク不正解析方法であって、ネットワーク上で伝送されているパケットを取り込むデータ収集工程と、階層化されたプロトコルに応じた階層化モジュールのパラメータを予め読み込んでおいたコンフィグレーションファイルで指定された情報に基づいて設定し、データ収集工程からのパケットを各階層化モジュールでフィルタリングしてパケットの細分化されたデータを元の単位に再構築することにより解析データを作成するデータ作成工程と、予め読み込んでおいたコンフィグレーションファイルで指定された内容を基にデータ作成工程からの解析データに不正が発生しているか判定するデータ解析工程とを備えるようにしている。

【0021】したがって、データ作成工程において、データ収集工程からのパケットを各階層化モジュールでフィルタリングしてパケットの細分化されたデータを元の単位に再構築することにより解析データを作成しているため、データ解析工程ではデータとして意味のある再構築後の解析データが解析対象となる。このため、データ部分に発生した不正を容易に判別することができる。

【0022】特にネットワークにおける不正はデータ部分に発生することが多いので、このデータ部分の解析を行うことが有効であるが、ネットワーク上で伝送されているパケットではデータ部分が細分化されているので、このデータ部分に不正が発生したかを判定するのは困難である。これに対し、本発明では再構築後の意味のあるデータを解析対象としているのでデータ部分に不正が発生したかを容易に判定することができる。

【0023】また、請求項2記載の発明は、情報通信ステーションの間で階層化されたプロトコルにより通信を行うように構築されたネットワークにおける不正を解析するネットワーク不正解析装置であって、ネットワ

ーク上で伝送されているパケットを取り込むデータ収集部と、階層化されたプロトコルに応じた階層化モジュールのパラメータを予め読み込んでおいたコンフィグレーションファイルで指定された情報に基づいて設定し、データ収集部からのパケットを各階層化モジュールでフィルタリングしてパケットの細分化されたデータを元の単位に再構築することにより解析データを作成するデータ作成部と、予め読み込んでおいたコンフィグレーションファイルで指定された内容を基にデータ作成部からの解析データに不正が発生しているか判定するデータ解析部とを備えるようにしている。

【0024】したがって、データ作成部において、データ収集部からのパケットを各階層化モジュールでフィルタリングしてパケットの細分化されたデータを元の単位に再構築することにより解析データを作成しているの

で、データ解析部ではデータとして意味のある再構築後の解析データが解析対象となる。このため、データ部分に発生した不正を容易に判別することができる。

【0025】さらに、請求項3記載の発明は、情報通信ステーションの間で階層化されたプロトコルにより通信を行うように構築されたネットワーク上で伝送されているパケットを取り込むデータ収集手順と、階層化されたプロトコルに応じた階層化モジュールのパラメータを予め読み込んでおいたコンフィグレーションファイルで指定された情報に基づいて設定し、データ収集手順からのパケットを各階層化モジュールでフィルタリングしてパケットの細分化されたデータを元の単位に再構築することにより解析データを作成するデータ作成手順と、予め読み込んでおいたコンフィグレーションファイルで指定された内容を基にデータ作成手順からの解析データに不正が発生しているか判定するデータ解析手順とをコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体としている。

【0026】したがって、コンピュータで記録媒体に格納されたプログラムを読み取り、インストールすることによってあるいはそのままプログラムを実行することによって、ネットワーク伝送時にデータ部分に発生した不正を容易に判別することができる。

【0027】

【発明の実施の形態】以下、本発明の構成を図面に示す実施の形態の一例に基づいて詳細に説明する。図2に、本発明に係るネットワーク不正解析方法が適用されたネットワークシステムの一例を示す。

【0028】この図2において、符号1は構内ネットワーク（以下、「LAN」という）であり、このLAN1にはルータ2を介して緩衝帯ネットワーク3が接続されている。この緩衝帯ネットワーク3は、ルータ6を介して外部ネットワーク7に接続されている。

【0029】本実施形態ではLAN1は、複数のステーション（図示せず）と、これらステーションを結ぶネッ

トワーク（図示せず）と、外部に接続する外部接続回線11とからなる。この外部接続回線11はルータ2に接続されている。但し、LAN1としては上述のものに限られず、単一のステーションから成るものとする事もできる。

【0030】緩衝帯ネットワーク3は、本発明に係るネットワーク不正解析方法を実現するネットワーク不正解析システム50と、コモンバス51と、外部接続回線52、53とからなる。ネットワーク不正解析システム50はコモンバス51に接続されている。外部接続回線52はルータ2とコモンバス51とを接続している。外部接続回線53はコモンバス51とルータ6とを接続している。

【0031】また、ネットワーク不正解析システム50は従来のネットワーク不正解析システムと同様にコンピュータシステムにて構成される。このコンピュータシステムは、特に図示していないが、例えば各種の演算処理を実行する中央演算処理装置と、演算処理を実行する上で必要なプログラムやデータ等を記憶する主記憶装置と、入出力ポート等の各種インタフェースと、このネットワーク不正解析システムを実現するプログラムやその処理を実行する上で必要な各種データや定数等を記憶する例えばハードディスクドライブ装置と、データや必要な指令を入力する入力装置と、中央演算処理装置で処理した結果を出力する出力装置とから構成されるのが一般的である。

【0032】図3に、本発明に係るネットワーク不正解析方法の実施の一形態を示す。この図3において、ネットワーク不正解析システム50は、中央演算処理装置が主記憶装置に記憶されたプログラムを処理することにより実現されるものであって、情報通信ステーションの間で階層化されたプロトコルにより通信を行うように構築されたネットワークにおける不正を解析するシステムである。すなわち、ネットワーク不正解析システム50は、例えば緩衝帯ネットワーク3で伝送されているパケットPTを取り込むデータ収集工程を実行するデータ収集部55と、データ収集部55からのパケットPTaを各階層化モジュールでフィルタリング及び再構築することにより解析データDTを作成するデータ作成工程を実行するデータ作成部56と、データ作成部56からの解析データDTに不正が発生しているか判定して解析結果CDCを出力するデータ解析工程を実行するデータ解析部57とから構成されている。

【0033】図1に、ネットワーク不正解析システム50の詳細構成を示す。この図1において、データ収集部55は、例えば緩衝帯ネットワーク3の間で伝送されているパケットPTを取り込むデータ収集処理部551と、このデータ収集処理部551のデータ収集処理を制御するデータ収集制御部552とから構成されている。データ収集処理部551は、収集したパケットPTをデ

ータ作成部56に供給する。

【0034】データ作成部56は、階層化されたプロトコルに応じた階層化モジュールのパラメータを、予め読み込んでおいたコンフィグレーションファイルで指定された情報に基づいて設定し、データ収集部55からのパケットPTaを各階層化モジュールでフィルタリングしてパケットPTaの細分化されたデータを元の単位に再構築することにより解析データDTを作成するデータ作成工程を実行するものである。

【0035】このデータ作成部56は、大別すると、階層化モジュール561と、これを制御し管理する制御管理部562とから構成されている。制御管理部562は、予め読み込んでおいたコンフィグレーションファイルで指定された情報に基づいて、階層化されたプロトコルに応じた階層化モジュール561のパラメータを設定できる。また、階層化モジュール561は、設定に基づいてデータ収集部55からのパケットPTaをフィルタリングしてパケットPTaの細分化されたデータを元の単位に再構築することにより解析データDTを作成できるようになっている。

【0036】階層化モジュール561は、1レイヤモジュール61₁、…、kレイヤモジュール61_k、…、Nレイヤモジュール61_Nからなる複数のレイヤモジュールから構成されている。ここで、Nは任意の整数であり、kは1～Nの間の任意の整数である。

【0037】1レイヤモジュール61₁は、読み込まれたコンフィグレーションファイルの内容に応じて、1レイヤフィルタ61_{1a}および1レイヤ再構築部61_{1b}が構成される。kレイヤモジュール61_kは、読み込まれたコンフィグレーションファイルの内容に応じて、kレイヤフィルタ61_{ka}およびkレイヤ再構築部61_{kb}が構成される。Nレイヤモジュール61_Nは、読み込まれたコンフィグレーションファイルの内容に応じて、Nレイヤフィルタ61_{Na}およびNレイヤ再構築部61_{Nb}が構成される。そして、各レイヤモジュール61₁、…、61_k、…、61_Nは、1からNまで順に処理される。

【0038】制御管理部562は、各レイヤモジュール61₁、…、61_k、…、61_Nにおいてデータを作成するデータ作成制御部62aと、各レイヤモジュール61₁、…、61_k、…、61_Nにおいてデータの記憶を制御するメモリ制御部62bと、解析データDTを出力させるためのアナライザ管理部62cとから構成されている。そして、制御管理部562は、1レイヤモジュール61₁、…、kレイヤモジュール61_k、…、Nレイヤモジュール61_Nをそれぞれ制御及び管理する。

【0039】データ解析部57は、予め読み込んでおいたコンフィグレーションファイルで指定された内容を基にデータ作成部56からの解析データDTに不正が発生しているか判定して解析結果CDCを出力するデータ解析工程を実行するものである。

【0040】このデータ解析部57には、アプリケーション層セッション単位のデータに不正があるかを解析するアプリケーションアナライザ570が設けられている。そして、このアプリケーションアナライザ570は、予め読み込んだコンフィグレーションファイルに記載されている内容に基づいてフィルタリング及び再構築されたデータDTに不正がないか否かを解析する。

【0041】図4に、コンフィグレーションファイルの例を示す。この図4において、コンフィグレーションファイル500は、データ作成部56からデータ解析部57に渡すデータDTの指定をするための情報やデータ解析部57で解析する情報を書き込むことができるようになっており、例えば図4に示すような内容を記載できるようになっている。

【0042】図5に、解放型システム間相互接続(OSI; Open System Interconnection)の7層モデルの例を示す。この図に示す階層化モデル800は、解放型システムの通信機能を7つに階層化したものであり、物理レイヤ801、データリンクレイヤ802、ネットワークレイヤ803、トランスポートレイヤ804、セッションレイヤ805、プレゼンテーションレイヤ806、アプリケーションレイヤ807に階層化されている。

【0043】物理レイヤ801は、ビット伝送に必要な物理的条件や電気的条件が定められている。データリンクレイヤ802は、データ伝送誤り制御手順等が定められている。ネットワークレイヤ803は、公衆パケット交換等各種通信網を介して両端のシステム間でデータのやりとりを可能とするためのものである。トランスポートレイヤ804は、両端のシステムの間で透過的で信頼性の高いデータ転送を行うためのものである。セッションレイヤ805は、両端のアプリケーションプロセスでの対話を効率よく行うため、同期をとったり伝送モードの選択、送信権の制御を行うためのものである。プレゼンテーションレイヤ806は、両端のアプリケーションプロセスが扱うデータを正確にかつ効率よく転送できるようにデータ形式を制御するためのものである。アプリケーションレイヤ807は、ユーザが実行する様々なアプリケーションに応じて、ファイル転送、メッセージ通信処理システム、下層端末、遠隔データベースアクセスなどのアプリケーションサービス要求を実行するためのものである。

【0044】このように構成されたネットワーク不正解析システム50の動作を図6～図8に説明する。図6に、同システム50の動作を説明するためのフローチャートを示す。図7、8に、同システムによって処理されるデータの内容の例を示す。

【0045】ここで、緩衝帯ネットワーク3のコモンバス51上を一つの意味有る情報ないしデータを構築する複数のデータパケット、例えば通信データ90a、90b、90c、90dが流れているとする。

【0046】これらの通信データ90a, 90b, 90c, 90dは、例えば図7に示すように受信先ID91a, 91b, 91c, 91dと、送信元ID92a, 92b, 92c, 92dと、順番93a, 93b, 93c, 93dと、データ94a, 94b, 94c, 94dとから構成されている。

【0047】このコモンバス51上の伝送される通信データ90aは、次のようにして構成されている。すなわち、例えば「I am a cracker.」というアプリケーションレイヤでのデータ95は細分化されて(ステップ(S)21)、「I am」というデータ94bと、「a c」というデータ94dと、「rac」というデータ94aと、「ker.」というデータ94cとに分割されたデータとなる。そして、さらに細分化されて(S22)、ヘッダを付けた通信データ90a, 90b, 90c, 90dにされ、これらは図5に示す階層化モデル800によりネットワーク上を伝送されることになる。緩衝帯ネットワーク3上でのデータ単位は、通信データ90a, 90b, 90c, 90dとなる。このデータ単位で、緩衝帯ネットワーク3のコモンバス51上を伝送されること

【0048】図6に示すように、ネットワーク不正解析システム50は、コンフィグレーションファイルを読み込む(S11)。これにより、データ作成部56の1レイヤモジュール61₁の1レイヤフィルタ61_{1A}及び1レイヤ再構築部61_{1B}, ..., kレイヤモジュール61_kのkレイヤフィルタ61_{kA}及びkレイヤ再構築部61_{kB}, ..., Nレイヤモジュール61_NのNレイヤフィルタ61_{NA}及びNレイヤ再構築部61_{NB}には、データ解析部57に渡すデータやフィルタリング及び再構築すべきデータに関するパラメータが設定される。また、このコンフィグレーションファイルにより、データ解析部57で解析する内容が設定される。

【0049】ここで、Nの値は、図5に示す階層化モデル800のどの階層までのデータとして再構築するかにより決定される。本実施形態では、N=7としてアプリケーション層セッション単位にまで再構築している。但し、N=7に限られず、例えばN=3としてネットワーク層セッション単位にまで再構築するようにもできる。いずれの場合もデータ解析に必要なセッション単位にまで再構築するように設定できる。

【0050】次に、データ収集部55は、データ収集制御部552の制御下に、コモンバス51の上を伝送されているパケットPTの1パケット(例えば通信データ90a)を取り込み(S12)、この1パケットがコンピュータシステムの主記憶装置またはハードディスクドライブ装置等にある作業エリアにコピーされる(S13)。これにより、この作業エリアにコピーされた1パケットは、階層化モジュール561の1レイヤモジュール61₁に取り込まれ、コンフィグレーションファイル

の情報に応じて1レイヤ目の処理を実行して次の層のレイヤモジュールに渡す(S14)。この1レイヤモジュール61₁では、パケットのヘッダ部のさまざまなフィールドの中の値と、コンフィグレーションファイルで指定されたフィルタ通過パラメータとの比較を行い、コンフィグレーションファイルで指定されているデータを選びだす処理を実行したり、通過処理したりする。また、フィルタ通過処理ではデータを変更しない。

【0051】次いで、1レイヤモジュール61₁の下層の各レイヤモジュールは、上述と同様にコンフィグレーションファイルの内容に応じてそれぞれ処理を実行する。

【0052】kレイヤモジュール61_kの前のモジュールが処理した結果をkレイヤモジュール61_kが受け取る。

【0053】ここで、各レイヤモジュール61₁, ..., 61_k, ..., 61_Nでは同様の処理が実行されるので、一例としてkレイヤモジュール61_kについて詳細に説明する。

【0054】kレイヤモジュール61_kは、予め読み込まれたコンフィグレーションファイルの情報に応じて、受け取ったデータをkレイヤフィルタ61_{kA}に通すのか否か、kレイヤ再構築部61_{kB}を動作させるのか否か、あるいは再構築あるいは非再構築のデータをデータ解析部57に渡すか否かのパラメータが設定されているので、そのパラメータの設定に従って処理を実行する(S15)。

【0055】例えば、コンフィグレーションファイルの情報の指定によって各パラメータが設定されているとすると、kレイヤモジュール61_kでは、上層のレイヤモジュールが処理した結果のデータをkレイヤフィルタ61_{kA}を通過させたのち(S151; YES)、そのデータを再構築する場合には(S152; YES)、バッファを使用して再構築し(S153)、アプリケーション層単位でのデータにまでの再構築が完了しない場合には(S154; NO)、kレイヤモジュール61_kを抜ける。そして、次のパケットを読み込む(S12)。

【0056】また、バッファを使用して再構築し(S153)、再構築が完了した場合(S154; YES)にはkレイヤ再構築部61_{kB}のバッファにデータが蓄えられている。この場合あるいはデータを再構築しない場合(S152; NO)には、再構築したデータをデータ解析部57に渡すタイミグになったときに(S155; YES)、kレイヤ再構築部61_{kB}のバッファに蓄えていたデータをデータ解析部57に渡す(S156)。また、データ解析部57に渡さないタイミグになったところで(S155; NO)、これより上側の層のレイヤモジュールにデータを渡す。

【0057】これにより、kレイヤモジュール61_kより上層のレイヤモジュールで処理された結果、図8に示

すように再構築されて(S23)、分割されたデータとして「rac」というデータ94aがデータ解析部57に渡る。

【0058】以上の処理を1パケット毎に繰り返すことにより(S13~S16)、ネットワーク上でのデータ単位のパケットPTは、図8に示すように再構築され(S23)、「I am」というデータ94bと、「ac」というデータ94dと、「rac」というデータ94aと、「ker.」というデータ94cとに分割されたデータとなる。さらに、再構築されて(S24)、「I am ac racker.」というアプリケーションレイヤでの元のデータ95にされる。

【0059】下位の層のレイヤモジュールが上記のようにコンフィグレーションファイルの情報によって各パラメータが設定されているとすると、Nレイヤフィルタ61にまでデータが渡る。

【0060】Nレイヤフィルタ61では、上述と同様にコンフィグレーションファイルの情報により設定されたパラメータで受け取ったデータの処理を行い、解析データDTとしてデータ解析部57に渡す(S16)。

【0061】また、このフローチャートを使用すれば、複数の種類のフィルタを設定することにより複数の種類のクラッキング等の不正アクセスを同時に監視できる。

【0062】データ解析部57では、アプリケーションアナライザ570が予め読み込んでおいたコンフィグレーションファイルで指定された内容を基にデータ作成部56からの解析データDTに不正が発生しているか判定している。このアプリケーションアナライザ570の判定した結果は、例えばディスプレイ上に、図9に示すような画面900として表示される。

【0063】ここで、アプリケーションアナライザ570は、不正解析処理を次のいずれか一方あるいは双方を採用するようにしている。但し、これらの処理方法に限られないのは勿論である。

【0064】(i)注目しているプロトコルでどのような操作をすれば、不正が実行可能かを調べておき、その手順をアプリケーションアナライザ570用のコンフィグレーションファイルに記述しておき、解析データDTとコンフィグレーションファイルに記載された手順を比較して一致すれば、その通信は不正なものであると判断処理を実行する。

【0065】(ii)セキュリティを確保するために厳重に管理する必要があるファイルやプログラム等をアプリケーションアナライザ570用のコンフィグレーションファイルに記載しておき、記載しておいたリソースに変化があった時点で、その通信は不正なものであると判断処理を実行する。

【0066】上述したネットワーク不正解析システム50によれば、例えば次のような不正(クラッキング)を防止できる。

【0067】(1)TCPプロトコルのシーケンス番号を推測し、偽のセッションを確保し攻撃対象ホストのファイルに不正アクセスすること。

【0068】(2)SMTPプロトコルのDEBUGコマンドを使い、攻撃対象ホストのファイルに不正にアクセスすること。

【0069】(3)MIMEを使って攻撃ホストのセキュリティ管理ファイルを書換え、攻撃ホストにパスワード無しでログインできるようにすること。

【0070】(4)電子メールやニュースを攻撃対象ホストの処理能力を超えて大量に送りつけ、ネットワーク機能を麻痺させること。

【0071】(5)telnetプロトコルで、root,quest等めばしいアカウントにアクセスし、パスワードを適当に推測し、ログインを試みること。

【0072】(6)TFIPプロトコルを用いて、パスワード無しで攻撃対象ホストのファイルにアクセスすること。

【0073】以上のように構成された本実施形態のネットワーク不正解析システム50によれば、次のような利点がある。

【0074】(1)アプリケーション層までのセッションの再構築を行うことができ、不正解析をおこなう者にとってわかり易いデータを取り扱えるようになった。すなわち、ネットワーク上でのパケットでのデータは細分化されているため解析を行うことが困難であるが、本実施形態のネットワーク不正解析システム50ではアプリケーション層までのセッションの再構築を行っているので解析データを意味有るデータとすることができ。これにより、データ中の不正の有無を容易に判定することができる。しかも、ネットワークでの不正の多くはデータ部分に発生するので、このデータ部分の不正を検出することにより効率の良い不正解析を行うことができる。

【0075】(2)層毎の完全なモジュール化により、複数の種類のプロトコルを扱えるようになった。すなわち、ネットワークのプロトコルは図5に示す階層化モデル800のようにモデル化でき、本実施形態のネットワーク不正解析システム50はコンフィグレーションファイルの設定に基づきこのモデルを利用して不正の解析を実行するので、新たなプロトコルが開発されても、コンフィグレーションファイル及びデータ作成部56の新たなプロトコルが対応する層を担当する一部のレイヤモジュールのみを変更することにより対応することができる。このため、データ作成部56を新たに開発されたプロトコルに対応させるためにデータ作成部56の全体を変更する必要はないので、プロトコル数の増大に容易に対応することができる。

【0076】(3)データ解析部での不正解析はコンフィグレーションファイルに記述した検知方法に基づいて行われるので、新たな種類の不正の発生をコンフィグ

ーションファイルの記述を変更するのみでデータ解析部のソフトウェア自体を変更することなく検出することができる。

【0077】(4) 緩衝帯ネットワーク3との組み合わせにより、任意の通信を取り扱えるようになった。例えば、LAN1のステーションや外部ネットワーク7が複数ある場合に、任意の送信元と受信先について不正解析を行うことができる。

【0078】(5) 緩衝帯ネットワーク3としてホストから独立しているので、ホスト数の増加にも容易に対応できる。

【0079】なお、上述の実施形態は本発明の好適な実施の一例ではあるがこれに限定されるものではなく本発明の要旨を逸脱しない範囲において種々変形実施可能である。例えば、図10に示すように、ネットワーク不正解析システム50に複数のネットワークインターフェースを設けてマルチホーム化することができる。例えば2つのネットワークインターフェースを有して別個のネットワーク4、5に接続されるときは、LAN1と外部ネットワーク7との間の通信は必ずネットワーク不正解析システム50の内部を通過することになる。このため、ネットワーク不正解析システム50でのパケットの収集を取りこぼし無く行うことができる。これにより、ネットワークでの不正を高精度に検出することができる。

【0080】また、図11に示すように、ネットワーク不正解析システム50をマルチホーム化すると共に、データ解析部57からデータ収集部55へ解析結果をフィードバックさせるようにしても良い。なお、図11では、データ作成部56及びデータ解析部57の具体的な図示は省略している。この場合、データ解析部57の解析結果によってデータ収集部55の処理が変化される。これにより、解析の結果、不正行為が行われているセッションやホスト等が特定できた場合、その通信についてはネットワーク不正解析システム50内を通過させないようにデータ収集部55を制御することができる。したがって、ネットワークでの不正のLAN1への侵入を防止することができる。

【0081】さらに、図12に示すように、データ作成部56を、層構造のレイヤフィルタ61_{1A}, ..., 61_{kA}, ..., 61_{nA}を有するフィルタリング処理部58と、層構造のレイヤ再構築部61_{1B}, ..., 61_{kB}, ..., 61_{nB}を有する再構築処理部59とを備えたものにする。この場合、データ作成部56では、フィルタリング処理部58においてフィルタリング処理をレイヤの数だけ先にまとめて行い、その後、再構築処理部59において各レイヤについての再構築処理を行う。このため、解析の対象にならないデータがより早く破棄されるため、不必要な再構築処理やメモリ占有が解消され、ネットワーク不正解析システム50の動作の高速化を図ることができる。

【0082】また、上述した各実施形態ではネットワーク不正解析システム50は図示しないコンピュータシステムから構成されるものとしているが、これには限られない。例えば、上述したネットワーク不正解析方法のデータ収集工程とデータ作成工程とデータ解析工程とをコンピュータに実行させるためのプログラムを記録したCD-ROMやフロッピーディスク等のコンピュータ読み取り可能な記録媒体を使用して汎用コンピュータを動作させることによりネットワーク不正解析システムを実行することもできる。

【0083】ここでのプログラムは、具体的には、情報通信ステーションの間で階層化されたプロトコルにより通信を行うように構築されたネットワーク上で伝送されているパケットを取り込むデータ収集工程を実行するデータ収集手順と、階層化されたプロトコルに応じた階層化モジュールのパラメータを予め読み込んでおいたコンフィグレーションファイルで指定された情報に基づいて設定し、データ収集手順からのパケットを各階層化モジュールでフィルタリングしてパケットの細分化されたデータを元の単位に再構築することにより解析データを作成するデータ作成工程を実行するデータ作成手順と、予め読み込んでおいたコンフィグレーションファイルで指定された内容を基にデータ作成手順からの解析データに不正が発生しているか判定するデータ解析工程を実行するデータ解析手順とをコンピュータに実行させるためのものである。

【0084】また、上述した実施形態ではデータ収集工程とデータ作成工程とデータ解析工程とを汎用コンピュータに実行させているが、これには限られずこれらの工程を専用のコンピュータから成る独立した装置に実行させるようにしても良い。さらに、上述した実施形態では、これらデータ収集工程とデータ作成工程とデータ解析工程とをコンピュータに実行させているが、これには限られずこれらの工程をシーケンス回路に実行させるようにしても良い。いずれの場合も、データ作成工程においてデータ収集工程からのパケットを各階層化モジュールでフィルタリングしてパケットの細分化されたデータを元の単位に再構築することにより解析データを作成するので、データ解析工程ではデータとして意味のある再構築後の解析データを解析対象とすることができる。このため、データ部分に発生した不正を容易に判別することができる。

【0085】

【発明の効果】以上説明したように、請求項1の発明のネットワークにおける不正を解析する方法によると、データ作成工程においてデータ収集工程からのパケットを各階層化モジュールでフィルタリングしてパケットの細分化されたデータを元の単位に再構築することにより解析データを作成して、データ解析工程ではデータとして意味のある再構築後の解析データを解析対象とすること

ができるので、データ部分に発生した不正を容易に判別することができる。

【0086】特にネットワークにおける不正はデータ部分に発生することが多いので、このデータ部分の解析を行うことが有効であるが、ネットワーク上で伝送されているパケットではデータ部分が細分化されているので、このデータ部分に不正が発生したかを判定するのは困難である。これに対し、本発明では再構築後の意味のあるデータを解析対象としているのでデータ部分に不正が発生したかを容易に判定することができる。

【0087】また、請求項2記載の発明のネットワークにおける不正解析装置によると、データ作成部においてデータ収集部からのパケットを各階層化モジュールでフィルタリングしてパケットの細分化されたデータを元の単位に再構築することにより解析データを作成して、データ解析部ではデータとして意味のある再構築後の解析データを解析対象とすることができるので、データ部分に発生した不正を容易に判別することができる。

【0088】さらに、請求項3記載の発明の記録媒体によれば、上述のデータ収集手順とデータ作成手順とデータ解析手順とをコンピュータに実行させるためのプログラムを任意のコンピュータに読み取らせて実行させているので、データ作成手順において、データ収集手順からのパケットを各階層化モジュールでフィルタリングしてパケットの細分化されたデータを元の単位に再構築することにより解析データを作成して、データ解析手順ではデータとして意味のある再構築後の解析データを解析対象とすることができる。このため、データ部分に発生した不正を容易に判別することができる。

【0089】したがって、請求項1から3のいずれかに記載した発明によれば次のような効果を得ることができる。

【0090】(1) アプリケーション層等の任意の層までのセッションの再構築を行うことができ、不正解析をおこなう者にとってわかり易いデータを取り扱えるようになった。すなわち、ネットワーク上でのパケットでのデータは細分化されているため解析を行うことが困難であるが、本実施形態のネットワーク不正解析システムではアプリケーション層までのセッションの再構築を行っているので解析データを意味有るデータとすることができる。これにより、データ中の不正の有無を容易に判定することができる。しかも、ネットワークでの不正の多くはデータ部分に発生するので、このデータ部分の不正を検出することにより効率の良い不正解析を行うことができる。

【0091】(2) 層毎の完全なモジュール化により、複数の種類のプロトコルを扱えるようになった。すなわち、ネットワークのプロトコルは図5に示す階層化モデルのようにモデル化でき、データ作成工程若しくはデータ作成部ではコンフィグレーションファイルの設定に基

づきこのモデルを利用して解析データを作成するので、新たなプロトコルが開発されても、コンフィグレーションファイル及びデータ作成工程若しくはデータ作成部の新たなプロトコルが対応する層を担当する一部のレイヤモジュールのみを変更することにより対応することができる。このため、データ作成工程若しくはデータ作成部を新たに開発されたプロトコルに対応させるためにデータ作成工程若しくはデータ作成部の全体を変更する必要はないので、プロトコル数の増大に容易に対応することができる。

【0092】(3) データ解析工程若しくはデータ解析部での不正解析はコンフィグレーションファイルに記述した検知方法に基づいて行われるので、新たな種類の不正の発生をコンフィグレーションファイルの記述を変更するのみでデータ解析工程若しくはデータ作成部のソフトウェア自体を変更することなく検出することができる。

【0093】(4) 緩衝帯ネットワークとの組み合わせにより、任意の通信を取り扱えるようになった。例えば、LANのステーションや外部ネットワークが複数ある場合に、任意の送信元と受信先とについて不正解析を行うことができる。

【0094】(5) 緩衝帯ネットワークとしてホストから独立しているので、ホスト数の増加にも容易に対応できる。

【図面の簡単な説明】

【図1】本発明のネットワーク不正解析方法が適用されたネットワーク不正解析システムの実施の形態を示すブロック図である。

【図2】ネットワーク不正解析システムとネットワークとの接続を示すブロック図である。

【図3】ネットワーク不正解析システムの実施の形態の概略を示すブロック図である。

【図4】同実施の形態で使用するコンフィグレーションファイルの例を示す説明図である。

【図5】同実施の形態にプロトコルの階層化の例を説明するための図である。

【図6】同実施の形態の動作を説明するためのフローチャートである。

【図7】同実施の形態の動作を説明するための図である。

【図8】同実施の形態の動作を説明するための図である。

【図9】同実施の形態で処理した結果を示す図である。

【図10】ネットワーク不正解析システムの他の実施形態を示すブロック図である。

【図11】ネットワーク不正解析システムの別の実施形態を示すブロック図である。

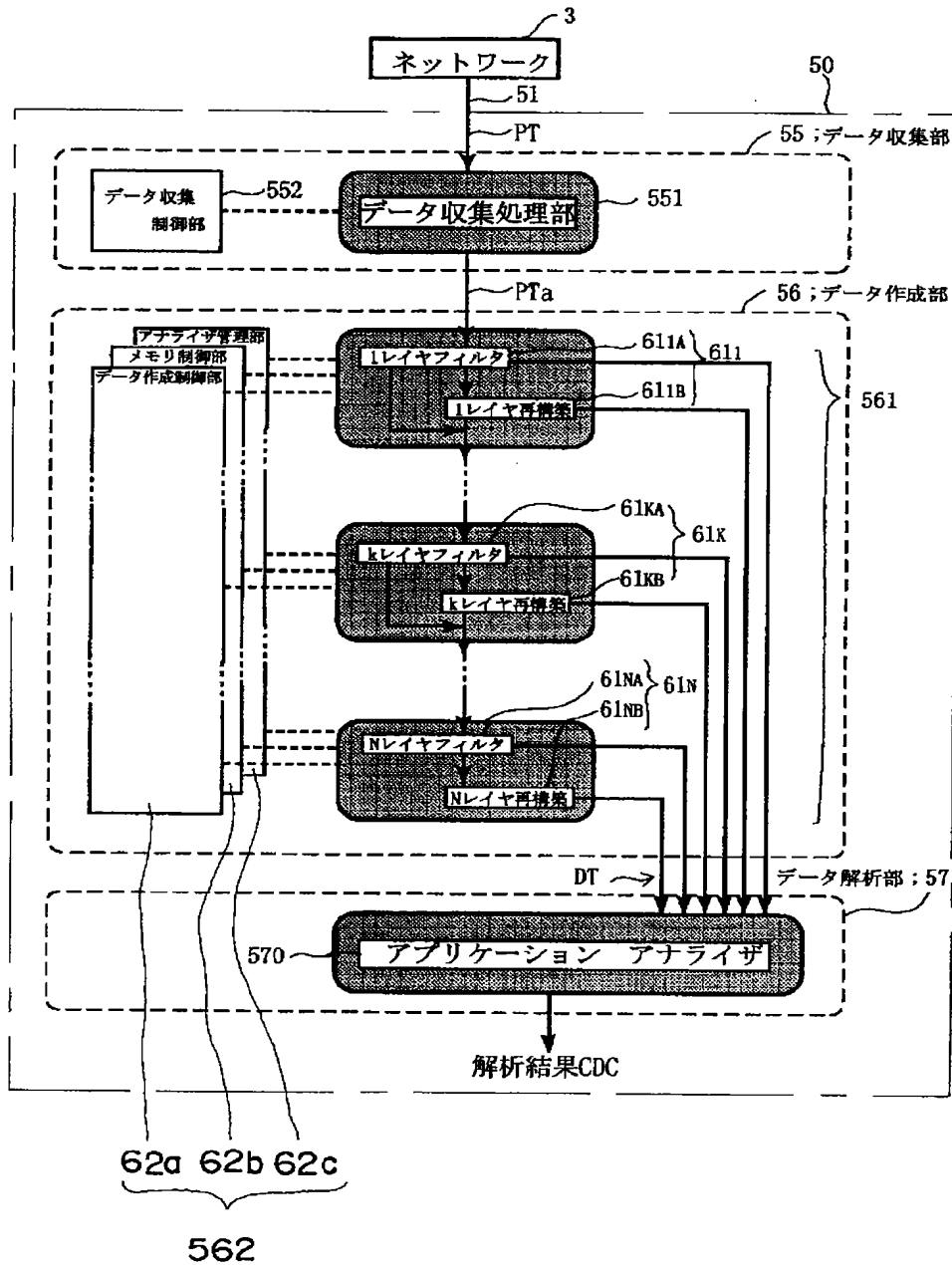
【図12】ネットワーク不正解析システムのさらに他の実施形態を示すブロック図である。

【符号の説明】

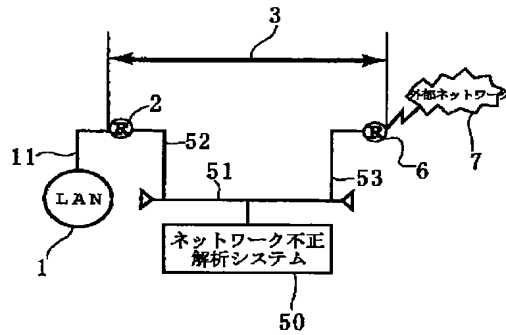
- 1 LAN
3 緩衝帯ネットワーク
7 外部ネットワーク

- * 50 ネットワーク不正解析システム
55 データ収集部
56 データ作成部
* 57 データ解析部

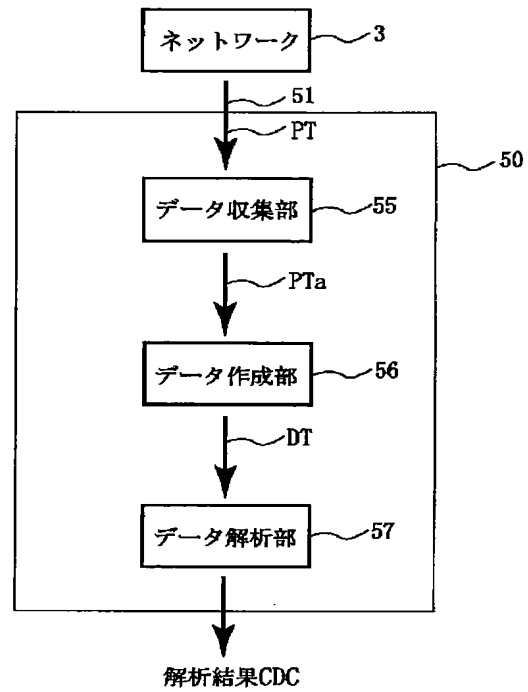
【図1】



【図2】



【図3】



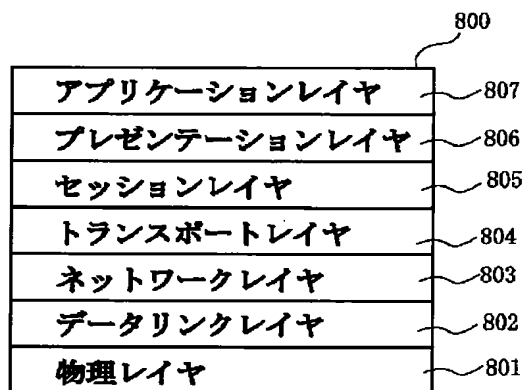
【図4】

```

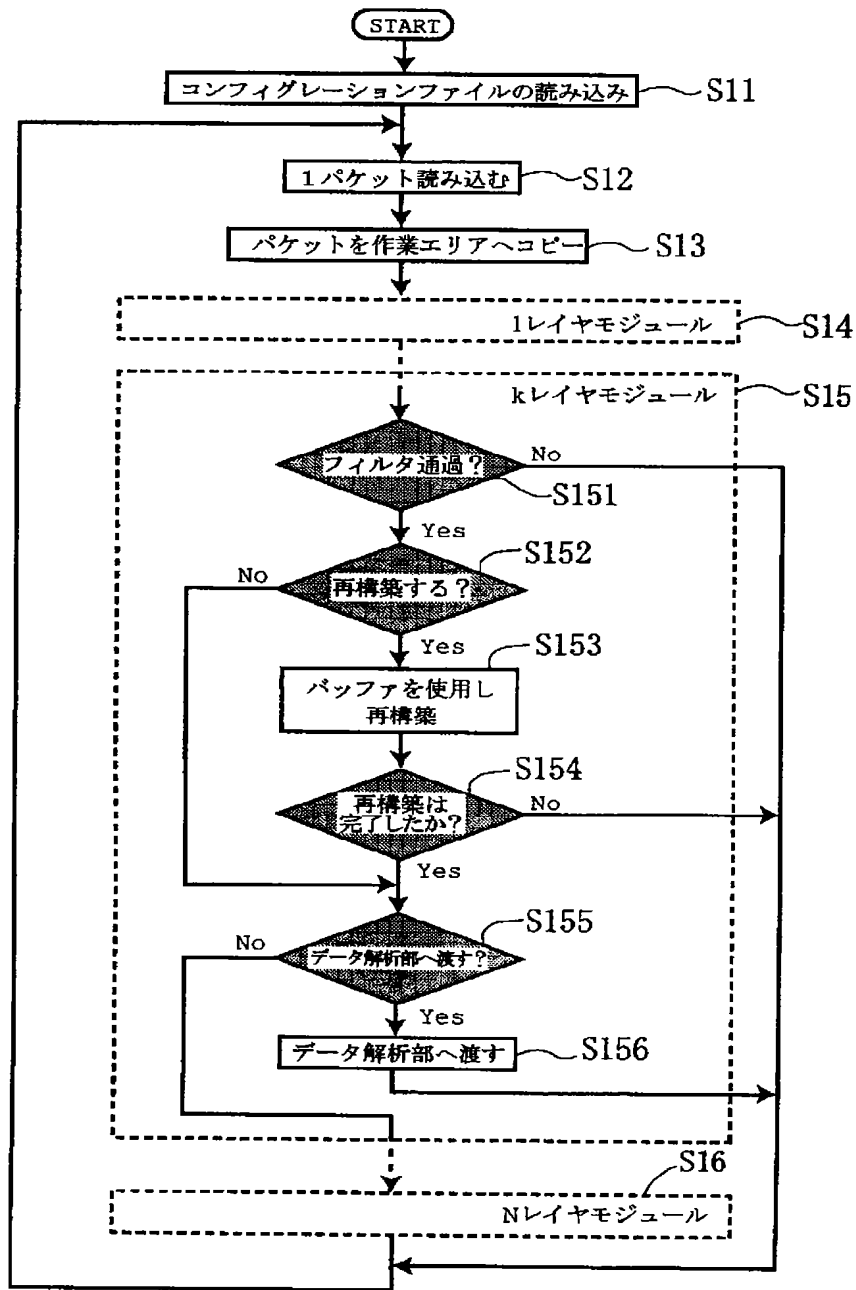
500
#-----#
# Filter for login Analyzer                      #
#-----#
filterset {
  physical  = { ether: * <-> aa:bb:cc:xx:yy:zz }
  network   = { ip: * <-> 202.26.95.68 }
  transport = { tcp: * <-> 23 }
  analyzer  = { login-A login.conf -log login.log -dump login.dump }
}

```

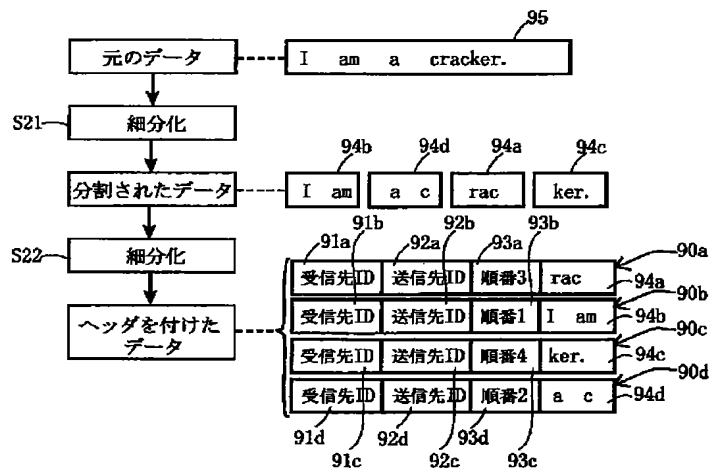
【図5】



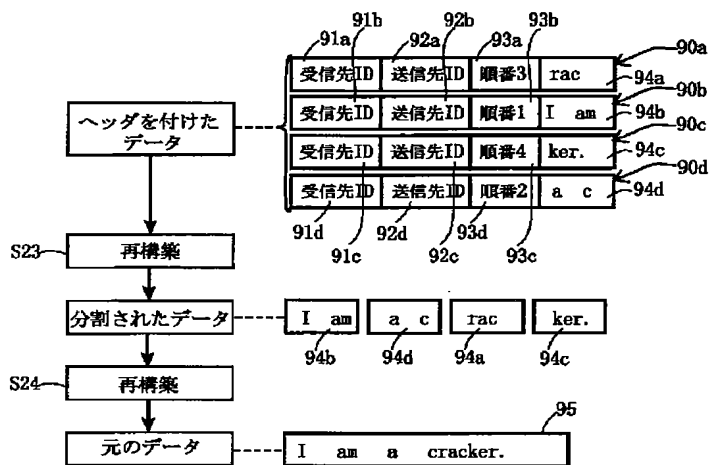
【図6】



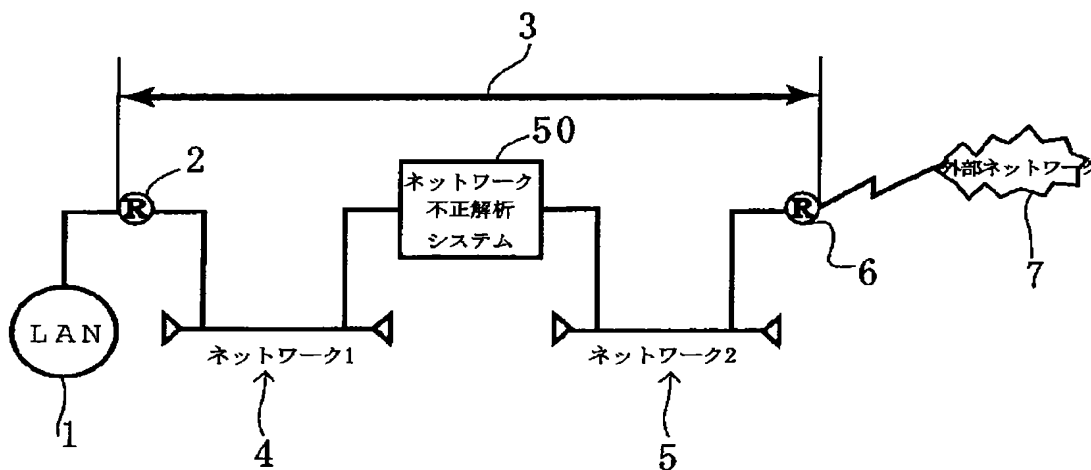
【図7】



【図8】



【図10】



【図9】

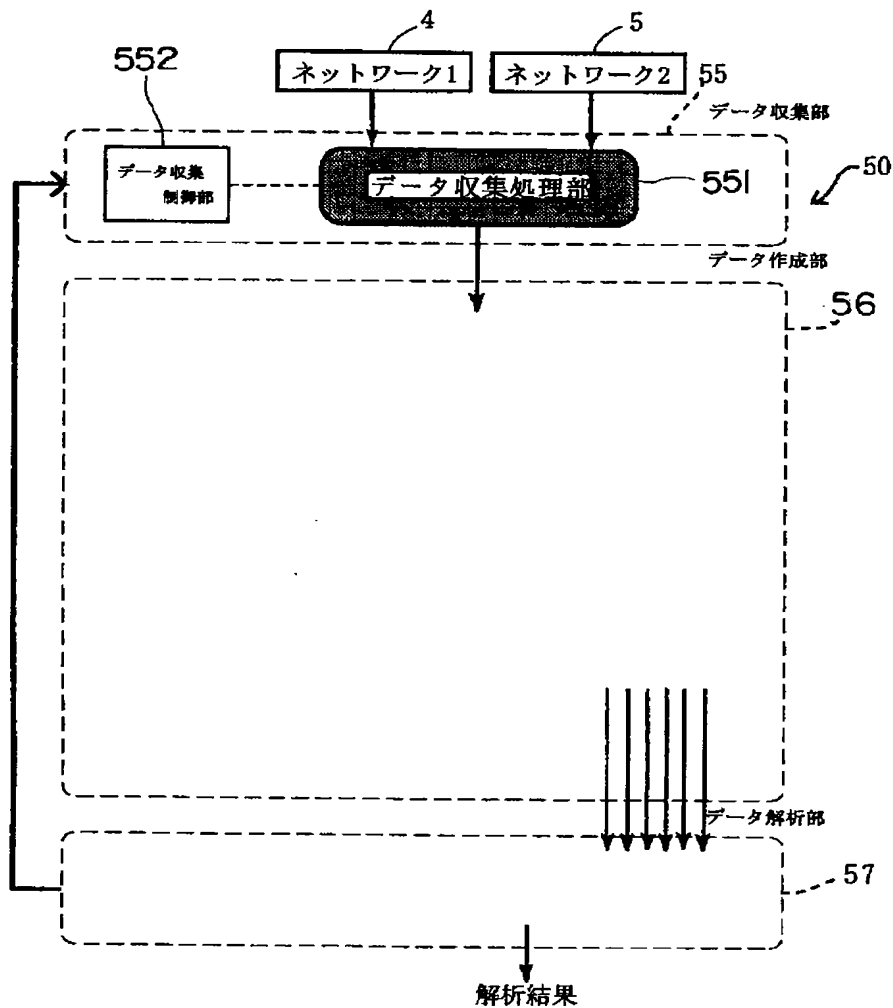
900

```

----- Cracking Data contents -----
Date           : Dec 26 13:28:00 1996
Server Address  : 202.26.95.68:23
Client Address  : 202.26.95.69:1024
Defhost Name    : host1
Login Times     : Threshold User = 0  Threshold System = 3
Easy Password Used : NO

----- Command Details -----
S :
S : Welcome to mail.nal.go.jp (tttyp4)
S :
S : login:
C : root
S : Password:
C : rootS
S : Login incorrect
S : login:
C : root
S : Password:
C : root
  
```

【図11】



【図12】

